MOODY'S ANALYTICS

WHITEPAPER

SEPTEMBER 2023


### Authors

**Alejandra Caro Rincon**, Associate Director
Alejandra.CaroRincon@moodys.com

**Gustavo Ordóñez**, Senior Director
Gustavo.Ordonez@moodys.com

### Contact Us

Americas
+1.212.553.1658
clientservices@moodys.com

Europe
+44.20.7772.5454
clientservices.emea@moodys.com

Asia (Excluding Japan)
+85 2 2916 1121
clientservices.asia@moodys.com

Japan
+81 3 5408 4100
clientservices.japan@moodys.com


# The impact of cyber security management practices on the likelihood of cyber events and its effect on financial risk


## Abstract

The rapid digitization of the economy and businesses' significant reliance on IT infrastructure has thrust cybersecurity to the forefront of risks to be actively managed. This trend has prompted investors, market participants, consumers, and regulators to address this emerging risk with greater urgency. Understanding a company's financial and technological exposure to cyber threats can help these market participants better prepare for potential cyber events and related financial losses. This study focuses on exploring the connection between a firm's cybersecurity management practices and the probability of a cyber event occurring. This study also examines the financial impact of these events by analyzing losses recorded over the 12-month period following a cybersecurity incident, and its potential effect on credit risk.

Our findings demonstrate a strong relationship between the quality of cybersecurity practices and the probability of a reported cybersecurity event. Certain industries, such as Finance, Healthcare, and Technology exhibit relatively higher risk of cyber related financial losses. Likewise, larger companies face an elevated risk of security events compared to smaller ones. This study also illustrates the significant negative effects of cyber incidents on firm value, with severe events leading to persistent negative equity returns over a 12-month period. Our findings demonstrate the potentially material financial implications of cyber risk, and highlight the importance of cybersecurity in a complete integrated risk assessment framework.

## Table of Contents

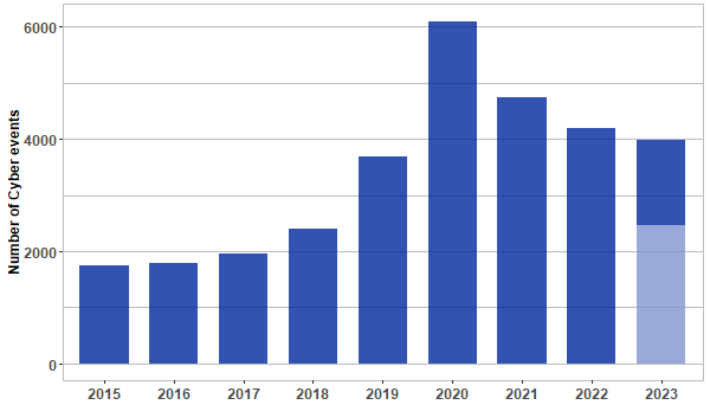
## 1. Introduction

The increased digitization of business and its reliance on IT infrastructure has exposed virtually every aspect of the economy to cyber risk. The pervasive and growing nature of cyber threats has made cybersecurity risk management a matter of paramount concern for corporate boards, regulators, investors, market participants, and consumers alike. In a recent survey of financial institutions, 87% of respondents reported that managing cybersecurity risk will be an extremely or very high priority over the next two years, the highest percentage of 16 priorities surveyed.[1]

As the frequency and severity of cyber-attacks continues to rise, the potential negative consequences on a company's financial performance and market value have become increasingly important considerations. However, due to the complex and multifaceted nature of cyber risk, it is difficult to assess its true financial impact. The lack of public disclosure of cybersecurity events and their resulting financial impact is a pervasive market issue. Companies often refrain from sharing information about cybersecurity incidents to protect their reputation and customer base, limiting accurate, comprehensive identification of cyber events.[2]

The rising number of cyber incidents has raised the attention of organizations and stakeholders alike. Figure 1 provides a compelling depiction of the increase of publicly disclosed incidents from 2015 to 2023, shedding light on the prevailing cyber risk landscape and its evolving implications. In just the past 5 years alone the number of publicly reported cyber incidents has doubled. The continuous upward trend in cyber incidents is emphasized by a notable peak in 2020, largely attributed to the disruptive impact of the COVID-19 pandemic.

Figure 1: Rising cyber-attack trend – reported events have doubled in the past 5 years




Note: Publicly disclosed cyber events dataset contains data from Jan 2015 to March 2023. Number of events in 2023 is projected based on the average monthly observation on the first quarter of the year and demoted in a lighter shade of blue.

The unique circumstances surrounding the pandemic contributed to the heightened cyber risk landscape. As organizations transitioned to remote work models, their average digital attack surface expanded significantly. The coexistence of corporate endpoints with a vast number of vulnerable consumer and Internet of Things devices within Work From Home-Remote networks introduced new and distinct cybersecurity risks compared to traditional in-office corporate networks.[3] As businesses gained a deeper understanding of these cyber threats, there was a noticeable decline in the frequency of such incidents after 2020.

In this article we examine the factors driving the probability and financial impact of cyber events. We investigate the relation between an organization's cyber security performance and the likelihood of cyber incidents occurring. Additionally, in observing the abnormal equity returns up to 12 months after a cyber event occurred, we assess the impact of these incidents on a firm's market value and credit risk factors.

[1] "Global Risk Management Survey, 12th Edition," Deloitte.

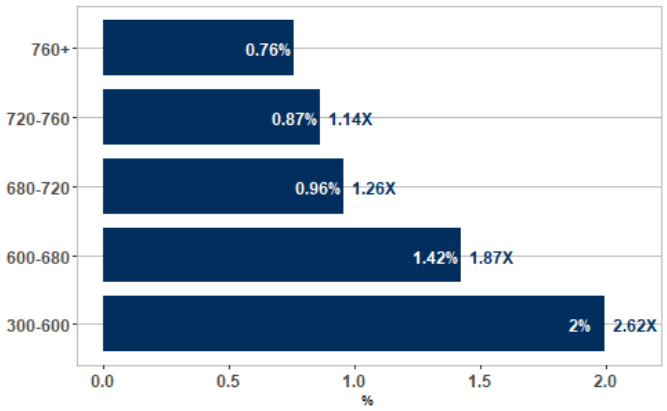
[2] On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) voted to adopt new cybersecurity requirements for publicly traded companies, creating new obligations for reporting "material" cybersecurity incidents and requiring more detailed disclosure of cybersecurity risk management, expertise, and governance. Companies will be required to disclose risks in their annual reports beginning on December 15, 2023.
U.S. Securities and Exchange Commission Press release 2023-139, accessed August 30, 2023. [https://www.sec.gov/news/press-release/2023-139]

[3] "Rush to Work from Home Exposes Alarming Security Issues," Bitsight, accessed June 14, 2023 [https://www.Bitsight.com/press-releases/rush-to-work-from-home-exposes-alarming-security-issues]

Our analysis encompasses the evaluation of monthly data from 2,571 public companies from 2015 to 2023. The results reveal a clear correlation between a decline in cyber security performance, as measured by the Bitsight cybersecurity rating (ranging from 250 to 900, with lower ratings indicating poorer performance), and a notable rise in the frequency of reported incidents. Further elaboration on this relationship can be found in section 3.

To illustrate this connection, we divided our sample into five percentiles based on the Bitsight cybersecurity rating. Figure 2 shows the percentage of reported events. The graph shows that Bitsight cybersecurity ratings strictly rank order the risk of cyber events, and demonstrates that companies in the quintile with the lowest ratings experience an incidence rate that is 2.6 times higher than that of the quintile with the highest ratings.

Figure 2: Poor cyber practices lead to 2.6x more Incidents

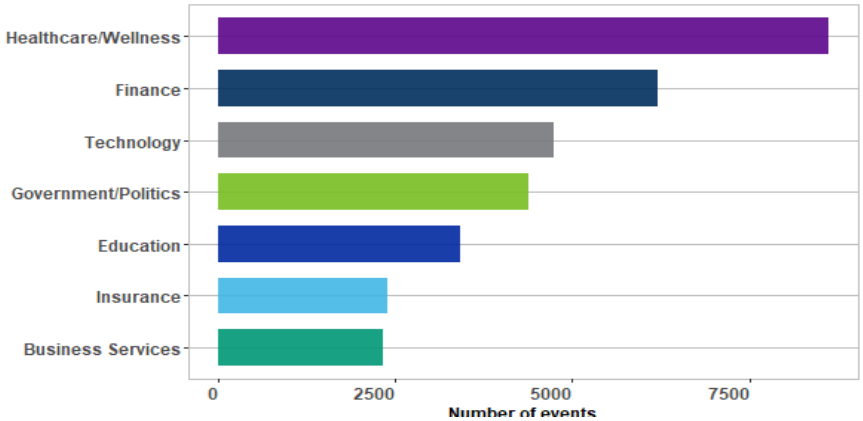



Percentage of reported incidents by cybersecurity rating bracket. Bitsight rates the cybersecurity performance of companies on a scale of 250 to 900, with the current achievable range being 300-820. Source: Bitsight and Moody's Analytics.

In our analysis, we demonstrate there are substantial, statistically significant, and persistent negative impacts of cyber incidents on firm value. Our findings show a robust association between cyber-attacks and abnormal equity returns, estimated through a market model. Specifically, our study reveals that moderate impact cyber events result in average abnormal equity returns ranging from -0.3% to -5.3% over a 12-month period (See section 2.2 for event study methodology description). These outcomes underscore the potentially significant financial consequences associated with cyber events and emphasize the urgency of implementing effective strategies for cyber risk management within companies.

Additionally, we examine variations of attacks across industry sectors, with finance, healthcare, and technology industries standing out as especially susceptible to attacks. Figure 3 offers an overview of reported events in the extensive dataset of publicly disclosed incidents.

Figure 3: Healthcare, Finance and Technology sectors under siege




Number of publicly disclosed cyber events by industry. Source: Bitsight

There are several potential reasons why companies in Healthcare, Technology, and Finance are more likely to be targeted by hackers. The primary factor is the significant value of data held by these sectors. They deal with vast amounts of sensitive

information, including financial records, personal health data, and intellectual property, which can be exploited for financial gain or other malicious purposes.

The Finance sector, in particular, attracts attacks like banking fraud, credit card theft, and ransomware. Healthcare is often a prime target due to its vast amount of sensitive personal data, including medical records, insurance details, and social security numbers, which hold significant value on the black market for identity theft, insurance fraud, and other illicit activities. The Technology sector, reliant on interconnected systems and networks, is highly vulnerable to cyber-attacks due to evolving technological advancements that introduce new exploitable vulnerabilities. Additionally, the sector's valuable intellectual property and trade secrets attract competitors and nation-states seeking advantages. The interconnectedness of technology infrastructure magnifies the potential impact of cyber-attacks, as compromising one system can have far-reaching consequences across multiple sectors.

Our research illuminates a distinct and direct correlation between a company's size and its vulnerability to cyber-attacks. This connection finds support through a positive and statistically significant coefficient embedded within the probabilistic model outlined in Section 4.1. Larger companies encounter heightened risks due to their relatively larger asset pools, a substantial customer base, and an extensive digital footprint. While smaller companies are not impervious to such threats, the magnitude and resources of larger organizations expose them to greater vulnerabilities, underscoring the imperative for robust cybersecurity measures to effectively mitigate these risks.

The remainder of the paper is structured as follows: Section 2 outlines the research methodology employed in this study, while Section 3 describes the data utilized. In Section 4, we present our empirical results that associate cyber security risk management practices and the probability of a cyber-related attack. In Section 5, we examine the impact of cyber events on firm value and credit risk. Finally, Section 6 concludes the paper by summarizing the main findings.

## 2. Methodology

The expected losses of a cyber event are defined as the product of the event's probability and the losses incurred once a cyber event has taken place:

$$Expected\ Loss = Probability\ of\ Event * Loss\ Given\ Event$$

For the probability of a cyber incident, we use a logistic model approach. This statistical modeling technique allows us to assess the likelihood of a cyber event occurring conditional on a set of firm characteristics. Secondly, for the losses associated with an observed cyber incident, we adopt an event-based methodology. This approach examines the deviation from expected equity returns that arises after a cyber incident occurs. In this section, we outline these methodologies in detail, providing insights into our approach for determining the expected losses.

### 2.1 Probability of a cyber event

In order to predict the probability of a cyber event and gain insights into the impact of the cybersecurity rating, a logit model is employed. This statistical method is well-suited for estimating binary outcomes pertaining to cyber events. By conducting an analysis of historical data and identifying pertinent factors, such as system vulnerabilities, user behaviors, and network configurations, the logit model is able to transform these variables into probabilities ranging from 0 to 1. This valuable information equips organizations with the ability to evaluate and manage their cybersecurity risks more effectively, facilitating the proactive allocation of resources and the mitigation of potential threats. Mathematically, the logit model can be represented as:

$$P(Cyber\ Event) = \frac{1}{1 + e^{-(\beta_0 + \beta_1 X)}}$$

The set of drivers, denoted by $X$, includes firmographic information such as industry, size, and cybersecurity performance. In section 3, we provide a detailed description of the data used and how it captures an organization's capacity to safeguard against cyber threats. The coefficients β capture the respective effects of these drivers on the probability of a cyber event, with the logistic function $e^{-(\beta_0 + \beta_1 X)}$ enabling the transformation of the linear combination into the desired probability estimate.

### 2.2 Event study methodology and financial impact of a cyber event

To evaluate the financial consequences of a cyber incident, we employ an event study approach. This methodology, widely utilized in financial econometrics (Campbell, Lo, MacKinlay, 1997), allows us to gauge the stock price's reaction to particular events, including corporate earnings releases, mergers and acquisitions, regulatory alterations, and other noteworthy developments. Our approach draws inspiration from the research conducted by Dwyer et al. (2022), where they assessed the repercussions of ESG controversies. We adopt a similar strategy to investigate the effect of cyber incidents.

Event studies rely on a robust theoretical framework that generates anticipated equity returns and serves as the foundation for comparing observed value fluctuations. Two pivotal assumptions in our approach encompass market efficiency and the forward-looking nature of market agents. The former assumes that stock prices swiftly react and accurately reflect all available information, while the latter posits that prices embody the expectations of market participants regarding future profits. These assumptions not only enable us to model expected returns but also provide us with a counterfactual scenario, illustrating what would happen if no additional information, such as a cyber event or an ESG controversy, were integrated into the market.

Expected equity returns are typically estimated using a market model calibrated on historical data, and are compared to observed returns over a specific time period. We run tests to evaluate whether the disparity between expected and observed returns is statistically significant. The difference between these two returns, expected and observed, is denoted as abnormal returns and is a key metric in our analysis. In Section 2.2.1 we provide further insight on the calculation of those elements of the model.

#### 2.2.1 Expected, observed and abnormal equity returns

In this study, we utilize a factor model to determine a firm's expected equity return based on its exposure to systematic risk factors (MacKinlay, 1997). Specifically, we focus on a single risk factor market model as shown in equation (1).

$$R_{i\tau} = \alpha_{it} + \beta_{it} MKT_{\tau} + \varepsilon_{i\tau}. \qquad (1)$$

Where $\beta_{it}$ represents the sensitivity of firm $i$ at time $t$ to a Market factor represented by $MKT_\tau$ [4] over a rolling window $\tau$. We estimate the model parameters over a 36-month rolling window, and conduct our analysis on a monthly basis, utilizing data on public firms from January 2015 to March 2023[5].

We compute abnormal equity returns as the difference between a firm's observed return and its expected equity return (equation 1). Once the rolling estimation window is completed, returns are calculated for multiple consecutive months using the previously estimated exposures. More specifically, the abnormal return ($AR$) is determined for each period ($t$, $t+1$,) $t+2$, etc.) as follows:

$$AR_{i,t+h} = R_{i,t+h} - \left(\hat{\alpha}_{it} + \hat{\beta}_{it} MKT_{t+h}\right), for\ h = 0, 1, 2, \dots, h \qquad (2)$$

where $\hat{\alpha}$ and $\hat{\beta}$ are the estimated coefficients from the rolling model in equation (1), and $h$ refers to the horizon from the time $t$ at which the abnormal return is observed. Cumulative abnormal returns ($CAR$) are the sum of $AR$ over a horizon of time $h$.

$$CAR_{i,t+h} = AR_{it} + AR_{i,t+1} + \cdots + AR_{i,t+h} \quad (3)$$

where for a given $CAR$ only one set of estimated exposure parameters is used, namely the ones estimated using observations until the month prior to the return period.

### 2.2.2 Impact on credit risk

We evaluate the effect of cyber events on credit risk using the concept of expected returns described in section 2.2.1. We calculate a firm's expected equity value $h$ months after an observed cyber event in period $t$ using the expected return derived from equation (1) and the firm's market value at the moment of the event, as shown in equation (4) below.

$$S_{t+h} = exp\left(\hat{R}_{i,t+h}\right) \cdot S_t \qquad (4)$$

While not directly observable, we can estimate the market value of the assets of a firm's using the stockprice $S_t$ . We achieve this by employing the estimation method proposed in Moody's Analytics' EDF™ structural credit risk model, as outlined by Nazeran and Dwyer (2015). We estimate the market value of the assets of a firm using the following relation:

$$A_t = S_t + L_t - DRP_t \qquad (5)$$

Where $A_t$ represent the market value of the asset at time $t$, $S_t$ is the equity, $L_t$ the liabilities and $DRP_t$ is a default risk premium that allows us to estimate the market value of the assets from their book value. Details of the full approach are given in (Pooya Nazeran, Dwyer, Douglas 2015)

These components are instrumental in defining the probability of default, $PD_t$. $PD_t$ is determined as the probability of the market value of assets falling below the value of the liabilities that must be paid, denoted as the default point $D$."

$$PD_t = Pr\ Pr\left[A_t \le D\right] = Pr\left[log(A_t) \le log\ (D)\right] \qquad (7)$$

$A_t$ is characterized by a stochastic process influenced by drift and volatility parameters. The estimation of the one-year Expected Default Frequency (EDF)[6] is described in equation (8) as:

$$EDF = M\left[\frac{log\left(\frac{A_0}{D}\right) + \left(\mu_A - \frac{1}{2}\sigma_A^2\right)}{\sigma_A}\right] \quad (8)$$

The observed and expected probabilities of default are calculated using the approach described in equations (5) to (8). In the case of equation 8 we allow for all the parameters to remain unchanged by the market asset value. In Figure 4 we present an example

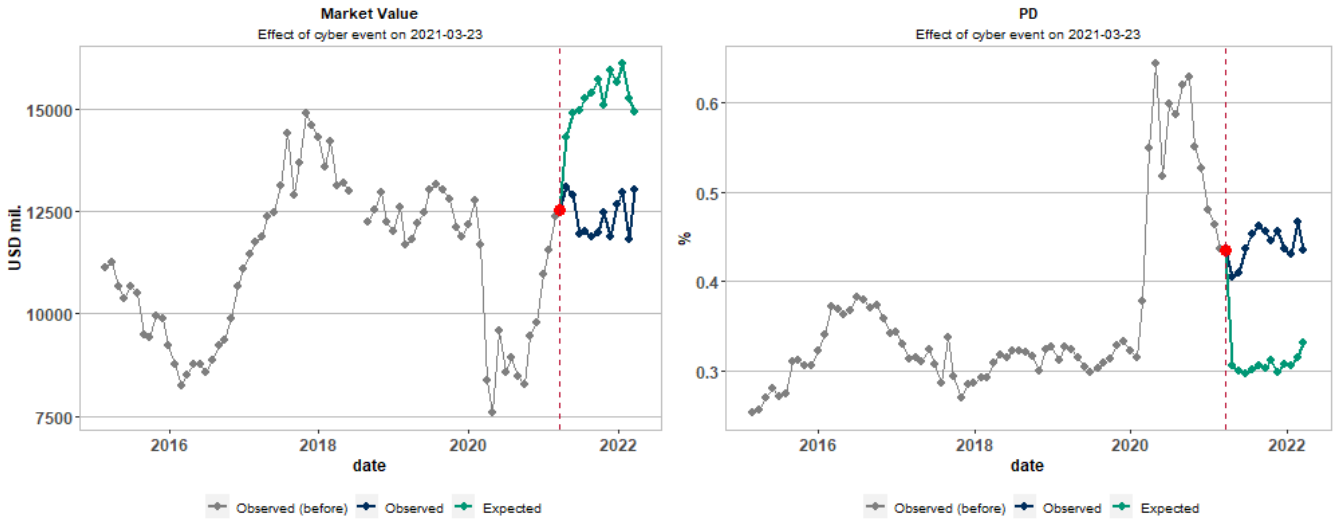
[4] We obtained the market return series from Kenneth French's website (https://mba.tuck.dartmouth.edu/pages/faculty/ken.french/data_library.html), the factors are presented at the regional level and comprise five regions: North America, Europe, Japan, APAC ex Japan, and emerging markets. The emerging market group include Brazil, Chile, China, Colombia, Czech Republic, Egypt, Greece, Hungary, India, Indonesia, Malaysia, Mexico, Pakistan, Peru, Philippines, Poland, Qatar, Saudi Arabia, South Africa, South Korea, Taiwan, Thailand, Turkey, United Arab Emirates. We associate each firm to the factor of the geography where its headquarters are located.

[5] All returns are log returns, and the regressions are estimated using OLS, requiring a minimum of 20 observations.

[6] EDF™ (Expected Default Frequency) is Moody's Analytics trademarked term for probability of default (PD).

of a company that experienced a ransomware attack in March 2021. This malicious cyber incident not only disrupted its system availability but also exposed the personal information of about 75,000 individuals. The figure consists of two graphs: one depicting the market cap on the left side and the other displaying the probability of default on the right side. The historical values leading up to the incident are depicted in gray, while the expected and observed values after the event are shown in green and blue, respectively. Following the incident, the observed market value significantly deviated from the expected value, which was initially projected to continue its upward trend. The substantial decline in market value following the cyber event consequently increased the credit risk for the company.

Figure 4: Realized and expected market value and probability of default after a severe cyber-event




## 3. Data

We combine two key sources of information: cyber risk and public company financial and credit risk data. Cybersecurity data provides valuable insights into organizations' security practices and is provided by Bitsight. Credit risk information is obtained from Moody's Analytics' CreditEdge™ data, and contains market and financial information for public companies encompassing debt, market capitalization, and forward-looking modeled probabilities of default for over 38,000 firms globally and over 11,000 default events over the past 50 years.[7] Our analysis covers monthly information from 2015 to 2023, allowing us to gain a comprehensive understanding of trends and developments during this timeframe.

### 3.1 Publicly disclosed cyber events and the Bitsight cybersecurity rating

We utilize publicly disclosed cyber events and security ratings from Bitsight to assess the cybersecurity status of companies. Bitsight collects information on data breaches and other security incidents from a large number of verifiable sources, including reputable news organizations and regulatory reporting (obtained via Freedom of Information Act requests or local equivalents). The publicly disclosed data encompasses a range of cyber-related incidents such as data breaches, crimeware, espionage, intrusion, ransomware, phishing attacks, and other security-related events. This dataset comprises over 45,000 records, corresponding to 28,000 events, with a single event potentially affecting multiple companies either directly or indirectly.

Bitsight categorizes cybersecurity events into four severity levels: Informational, Minor, Moderate, and Severe. The classification depends on the observed event and the number of affected users. Severity is determined by factors such as the number of records of personal information exposed, the type of event, and the company's size. This classification accounts for the higher risk baseline associated with larger companies.

Additionally, we use Bitsight cybersecurity ratings data. Bitsight's cybersecurity ratings are generated through the analysis of externally observable data, leveraging Bitsight's proprietary techniques to identify the scope of a company's entire digital

[7] The CreditEdge data set is a subset of the EDF-X solution, which contains information on over 450 million firms globally, including firm financials and prescored probabilities of default.

footprint. This data-driven approach requires no cooperation from the rated company. The rating is representative of the cybersecurity performance of an entire company, including its subsidiaries, business units, and geographic locations. The original dataset contains daily observations for more than 38,000 companies, from Jan 2025 to March 2023.[8] We conduct our analysis at the monthly level and limit it to public companies.

### 3.2 Public company risk and expected returns

We conducted an empirical analysis using publicly listed companies to develop a methodology for evaluating the impact of cyber-related incidents on company value and credit risk. Our research focused on companies that reported cyber events from January 2015 to March 2023. To gather relevant data, we accessed Moody's Analytics public company database to obtain monthly equity returns, which were cross-referenced with geographical matches on Kenneth French's website. Additionally, we used Moody's Analytics CreditEdge™ data for the same period. The data includes publicly traded firms information such as probability of default, market cap, calculated asset volatility and drift, and balance sheet and income statement line items. All returns considered in this study were firm-level monthly log returns.

To create a comprehensive dataset, we combined Bitsight's cybersecurity incident records with Moody's Analytics' equity returns data, resulting in 3,354 observations corresponding to 3,824 events across 1,542 distinct public firms. Our analysis was based on monthly data, with the awareness that certain firms experienced multiple attacks within the same month. To account for this, we considered the number of attacks per month but focused exclusively on the most severe incident recorded.

### 3.3 Descriptive Statistics

In our event studies, we examine both the short-term impact of cyber events by analyzing the expected and observed equity return during the month of the event, as well as the longer-term effect by assessing the return over a 12-month period starting at the event date. Table 1 presents the comprehensive return distributions for these time horizons.

Table1: Statistics on average monthly cumulative abnormal returns

| Month | PERCENTILE | | | | | | | | | MINIMUM | MAXIMUM | MEAN |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | | | |
| 1 | -0.10 | -0.06 | -0.04 | -0.02 | 0.00 | 0.01 | 0.03 | 0.06 | 0.10 | -0.61 | 0.68 | 0.00 |
| 2 | -0.15 | -0.09 | -0.06 | -0.03 | 0.00 | 0.02 | 0.05 | 0.08 | 0.13 | -0.92 | 1.00 | -0.01 |
| 3 | -0.19 | -0.12 | -0.07 | -0.04 | 0.00 | 0.03 | 0.06 | 0.10 | 0.17 | -1.19 | 1.02 | -0.01 |
| 4 | -0.23 | -0.14 | -0.08 | -0.04 | 0.00 | 0.03 | 0.07 | 0.12 | 0.19 | -1.90 | 1.28 | -0.01 |
| 5 | -0.26 | -0.16 | -0.10 | -0.05 | -0.01 | 0.03 | 0.08 | 0.13 | 0.22 | -2.19 | 1.38 | -0.02 |
| 6 | -0.28 | -0.17 | -0.10 | -0.05 | -0.01 | 0.03 | 0.08 | 0.13 | 0.25 | -2.65 | 1.61 | -0.02 |
| 7 | -0.31 | -0.19 | -0.12 | -0.06 | -0.01 | 0.03 | 0.08 | 0.15 | 0.27 | -2.99 | 1.66 | -0.02 |
| 8 | -0.33 | -0.21 | -0.13 | -0.07 | -0.02 | 0.03 | 0.08 | 0.16 | 0.28 | -3.04 | 2.20 | -0.02 |
| 9 | -0.36 | -0.22 | -0.14 | -0.07 | -0.01 | 0.03 | 0.09 | 0.18 | 0.31 | -3.24 | 2.13 | -0.03 |
| 10 | -0.38 | -0.23 | -0.14 | -0.07 | -0.02 | 0.04 | 0.10 | 0.19 | 0.33 | -3.24 | 2.39 | -0.02 |
| 11 | -0.41 | -0.26 | -0.15 | -0.08 | -0.02 | 0.04 | 0.11 | 0.19 | 0.34 | -3.24 | 2.17 | -0.03 |
| 12 | -0.42 | -0.27 | -0.16 | -0.09 | -0.02 | 0.04 | 0.11 | 0.20 | 0.36 | -3.24 | 2.16 | -0.03 |

In our data analysis, we made some noteworthy observations regarding cyber events reported by companies. While most firms typically disclose only one cyber event per month, some companies report four or more events within the same month. Furthermore, our analysis revealed that certain companies experienced an alarmingly high number of attacks, exceeding 40 incidents between January 2015 and March 2023. This highlights the fact that these companies are not only subject to frequent attacks but are also prime targets for cyber events.

To provide a clearer picture of these patterns, we present our findings in two tables. Table 2 presents the distribution of the number of attacks per company per month, shedding light on the frequency at which attacks occur for each company. Meanwhile, Table 3 offers a broader perspective by showcasing the distribution of attacks in general, providing valuable insights into their overall occurrence and impact.

Table 2: Distribution of number of events by firm and month

[8] For more detailed information on Bitsight's rating methodology, including data collection methods and underlying risk vectors, please refer to Bitsight (2023).

| Number of events per firm and month | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | Total |
|---|---|---|---|---|---|---|---|---|---|
| Number of companies | 3,021 | 239 | 67 | 18 | 5 | 2 | 1 | 1 | 3,354 |

Table 3: Distribution of number of events by firm reported between Jan 2015 and March 2023

| Number of Total events by company | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 - 40 | 41 - 104 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number of companies | 1,014 | 239 | 100 | 62 | 33 | 21 | 15 | 8 | 4 | 35 | 11 | 1,542 |

## 4. Results

In this section, we present the empirical findings of our analysis. Our study demonstrates that the probability of a cyber incident is influenced by various factors, including the company's implementation of robust cyber practices as measured by the Bitsight cybersecurity rating, as well as the industry and size of the firm. Specifically, larger companies face heightened targeting by malicious actors and are more vulnerable to potential errors made by employees, given their larger workforce. These factors can lead to the proliferation of open ports, spam, or phishing activities, consequently expanding the overall cyber-attack surface.

Furthermore, our analysis reveals statistically significant and negative average abnormal equity returns over a 12-month period following a cyber incident. These deviations from expected values indicate the adverse impact of cyber events on stock returns. Additionally, our investigation highlights that the diminished equity values resulting from cyber incidents can contribute to the subsequent deterioration of credit risk.

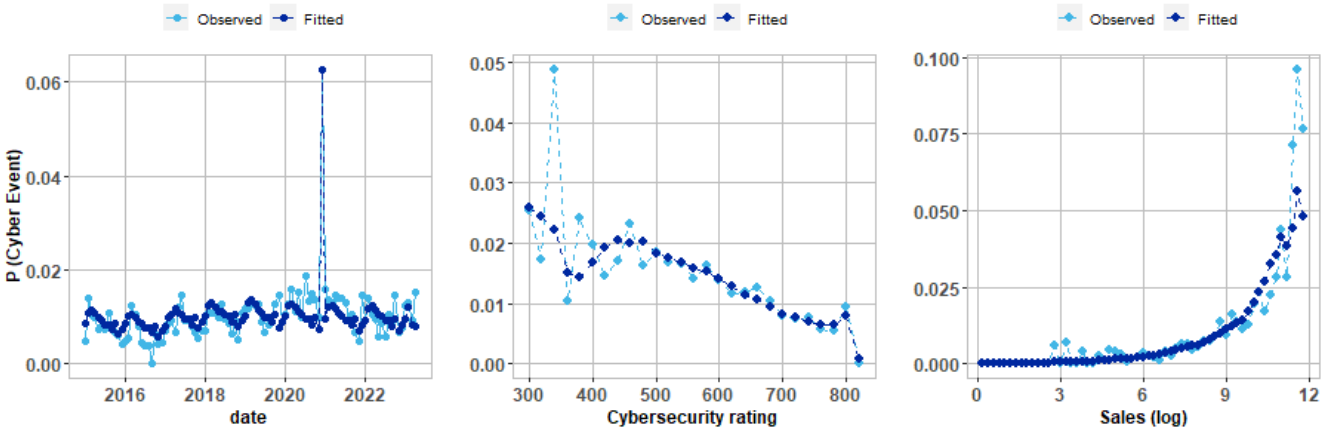
### 4.1 Probability of a cyber incident: companies with poorer cybersecurity performance are more vulnerable to cyber-attacks

Following the framework presented in Section 2.1, our empirical findings yielded significant insights into the probability of cyber events. Notably, the cybersecurity vector emerged as a crucial factor, demonstrating a negative and statistically significant coefficient.

Moreover, our investigation took into account industry variations, which revealed a significant impact on the likelihood of cyber events. Certain industries exhibiting a higher frequency of events or were more inclined to publicly disclose them. Table 4, detailed on the Appendix presents key elements of the model. Figure 6 visually presents the expected and observed probabilities of cyber events across different months, offering valuable insights into the temporal patterns and fluctuations of these events throughout the year.

Figure 6 illustrates the model's fit, as presented in Table 2, across various dimensions such as time, size, and cyber performance. The observed data is represented by the light blue line, while the darker blue line represents the fitted data. Overall, the model exhibits a good fit, although a few spikes in the data can be observed due to limited information availability. Figure 7, in the appendix, shows an accuracy of 80.2% which indicates the strong performance of the model described in table 5. The accuracy is measures by the area under the curve (AUC), which measures how well a classification model can distinguish between two categories (cyber event or non cyber event)

Figure 6: Observed and fitted probability by driver




Note: The spike in December 2020 represents an increase in the number of reported events that may have occurred prior to that. We account for such events.

Figure 8 illustrates the conditional probability of an incident based on the cyber score quantile. The probability increases in the lowest performance quantile (dark green), contrasting with the highest performance quantile (lime green). This finding suggests that as organizations improve their cybersecurity performance, the likelihood of experiencing an attack decreases.

Furthermore, our analysis revealed that larger companies are more susceptible to breaches. Figure 9 illustrates the probability of incidents based on company size, measured in dollar sales. Companies with sales exceeding 10 million dollars are more vulnerable

compared to those in the lowest sales bracket. This observation not only indicates that cyber criminals tend to target larger organizations but also emphasizes the added complexity associated with firm size and scale, and more complex IT systems in bigger companies.

Figure 8: Probability of a cyber incident by security score quantile

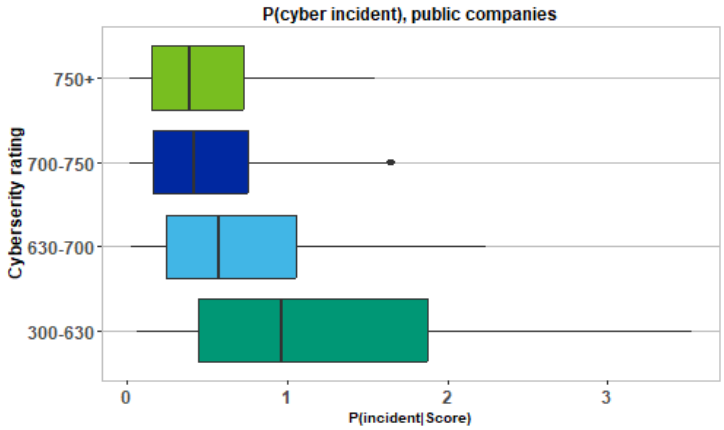
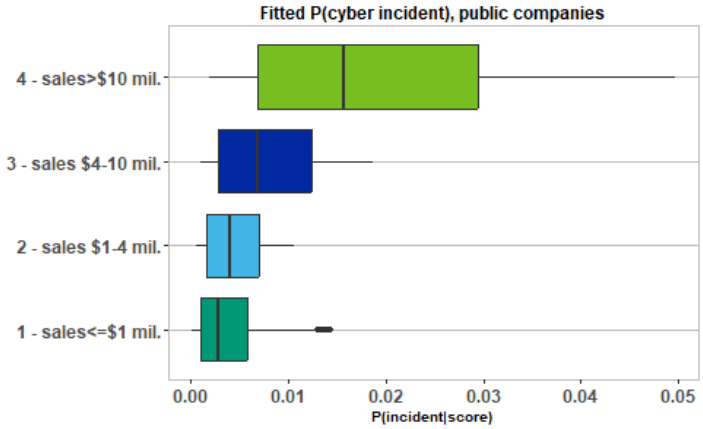



Figure 9: Probability of a cyber incident by size quantile




In Figure 10, in the appendix, we present the percentage of cyber incidents categorized by grade for each risk vector. The grades, ranging from A to F, represent percentiles within Bitsight's entire universe of rated firms, rather than the specific public company data sample we used in our study. Across several dimensions, we observe a consistent trend: stronger performance in a given dimension corresponds to a lower likelihood of reporting an incident. This pattern holds true for vectors such as botnet infections, desktop software, insecure systems, potentially exploited systems, and web application headers.

However, the relationship is not consistently monotonic for other vectors, particularly patching cadence. In contrast, we observe an apparently inverse trend for DKIM records and a relatively flat pattern for TLS SSL certificates and configuration. These findings highlight the nuanced relationships between performance grades and incident rates across different risk vectors, underscoring the need for a comprehensive understanding of each dimension's impact on cyber incident probabilities.

## 4.2 Cyber incidents may result in negative abnormal equity returns months after the event

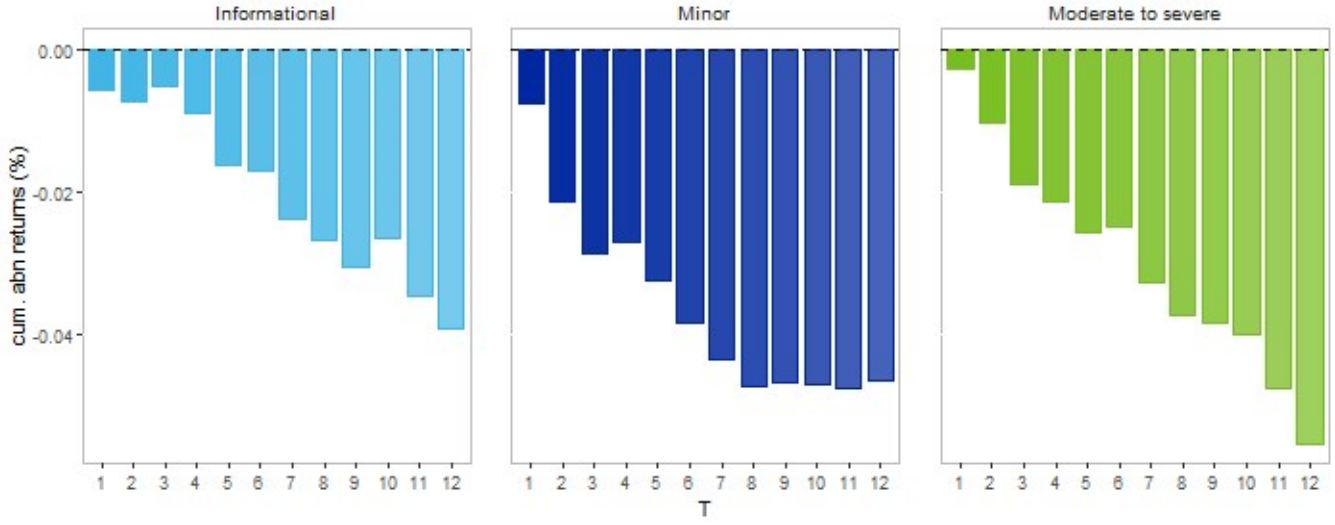
After evaluating the likelihood of an occurrence, our primary goal is to estimate its financial repercussions. Throughout the research described in this document we have observed that, on average, a cyber incident leads to a detrimental outcome that may endure for up to one year. Moreover, the severity of the incident exacerbates its impact. The relationship between these factors is depicted in Figure 11, which illustrates that the cumulative abnormal equity returns consistently sustain an influence well beyond the 12-month threshold following the cyber event. To determine the statistical significance of the average cumulative abnormal returns, we conduct a t-test as follows:

$$t_{Avg.CAR} = \frac{CAR}{SE_{Avg.CAR}},$$

Table 4 presents the impact of cybersecurity incidents on returns. The degree of severity in a cyber event is evaluated through a point scale established by Bitsight. Incidents accrue points based on several key factors, including the nature of the incident, the volume of data impacted, and the sensitivity of the compromised information[9]. During the 1-month period following the incident, the informational event type shows a mean cumulative abnormal return of -0.54%, the minor incident type has a slightly worse mean return of -0.674%, and the moderate to severe cases have a mean return of -0.28%. Moving to the 12-month mark, all event types exhibit significant negative returns. The informational event type has a mean return of -3.796%, while the minor event type experiences a larger decline with a mean return of -5.041%. As anticipated, the moderate to severe events demonstrate the most substantial decrease, with a mean cumulative return of -5.352%. In all cases, the high t-statistic suggests statistical significance with a confidence level of 1%.

It is important to note that although more severe events may not have an immediate negative impact, they tend to have the most significant detrimental effects in the long run. Overall, these findings indicate that the severity of the incident and the time elapsed since it occurred significantly influence the cumulative abnormal returns. Larger declines are observed for longer periods and more severe events. The t-values indicate the statistical significance of the mean returns.

Figure 11: Average cumulative abnormal returns up to 12 months after incident by severity classification



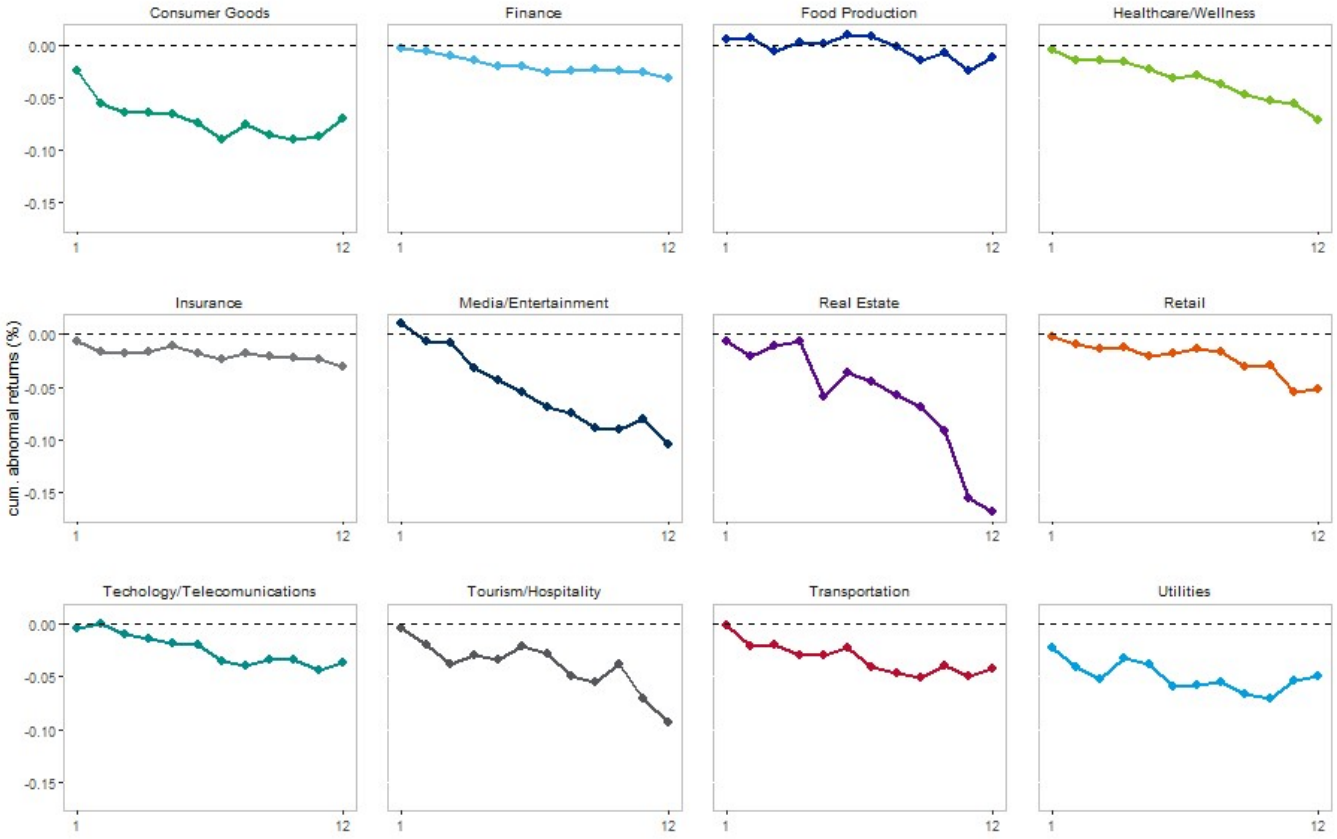

[9] Informational events predominantly encompass internal company incidents, such as DNS disruptions, where no personal information loss is recorded. Minor incidents, on the other hand, involve the loss of personal information for up to 100 individuals and are often linked to human errors or employee privilege misuse. In contrast, more severe events typically encompass instances of crimeware, espionage, and ransomware, involving the compromise of substantial amounts of data with malicious intent

Table 4: Average cumulative abnormal return by severity and months after cyber incident.

| Event type | N | mean | t |
|---|---|---|---|
| **1 - month after incident** | | | |
| Informational | 1395 | -0.54 % | -5.12089 |
| Minor | 680 | -0.674% | -3.11278 |
| Moderate to severe | 1308 | -0.28 % | -2.48496 |
| **2 - month after incident** | | | |
| Informational | 1377 | -0.678 % | -4.48888 |
| Minor | 669 | -2.084 % | -6.7019 |
| Moderate to severe | 1292 | -0.999 % | -6.20012 |
| **12- months after incident** | | | |
| Informational | 1247 | -3.796 % | -9.28625 |
| Minor | 610 | -5.041 % | -6.0334 |
| Moderate to severe | 1163 | -5.352 % | -12.2115 |

Moreover, our analysis reveals that the impact of incidents varies significantly across different industries. Notably, while the Finance, Healthcare, and Technology sectors are more frequently targeted by attacks, the average losses incurred in these industries are comparatively lower than those experienced by other sectors in our sample, such as Real Estate, Tourism, and Media and Entertainment. In other words, despite facing a higher frequency of attacks, the Financial, Healthcare, and Technology industries appear to have more effective security measures or are better equipped to mitigate the financial consequences of incidents. On the other hand, industries like Real Estate, Tourism, and Media and Entertainment seem to be more vulnerable, experiencing higher average losses even with a lower frequency of attacks. This insight underscores the importance of industry-specific risk management strategies and highlights the need for tailored security measures to address the unique challenges faced by different sectors. In the Appendix we also present results on the average number of cyber events across different industries as a function of the different attack vectors considered and the grades awarded by Bitsight.

Figure 12: Average 1-month to 12-months cumulative abnormal returns




## 4.3 Impact on credit risk: loss on stock value potentially leads to credit risk deterioration

Using the methodology described in Section 2.2.2, we can estimate how cyber events can be linked to abnormal returns in equity price. Focusing on the cases where we observe a negative abnormal return, that is, where the observed return is lower than expected, we can leverage Moody's EDF methodology to estimate the implied deterioration in credit risk. The intuition behind this approach is that a deterioration in stock price return (with respect to the expected return) implies a deterioration in the (market-implied) asset value return. This consequently implies that, under the lower observed return, the asset value of the firm comes closer to the default barrier than would have been expected. From this, we can estimate the impact of the abnormal return on the credit risk of the firm.

It is important to mention that it is difficult to isolate the impact of cyber events on changes in stock returns. In fact, it is often the case that observed returns are higher than expected, which suggests that other market forces may mask the negative impact of cyber events. Nevertheless, we are confident that negative abnormal returns are driven by these cyber events, since, as observed in Section Section 4.2, "moderate" and "severe" cyber events result in lower abnormal returns than when the cyber events are categorized as "informational" by BitSight.. On average, market losses contribute to a 0.18% increase in the probability of default after one month following the event, and a 0.24% increase after 12 months. Figure 13 illustrates the changes in the probability of default relative to the expected values at 1 and 12 months subsequent to a cyber event. To aid comprehension, the distribution is restricted to cases where the observed probability of default exceeds the expected value, and the results are presented in logarithmic differences. Instances where a favorable effect is observed can be attributed to concurrent market events exerting opposing influences.

Furthermore, it is noteworthy that the distribution of the 12-month increase in probability of default (PD) demonstrates a more pronounced rightward shift (depicted in light blue) compared to the distribution corresponding to the 1-month increase (depicted in darker blue). This observation highlights that changes in asset value can have enduring implications for credit risk up to one year after the occurrence of a cyber event.

We also extend our analysis to the industry level, focusing on selected industries. Consistent with our findings in Figure 12, we note that the impact on credit risk not only varies over time but also across industries. Interestingly, the results indicate that industries

heavily targeted, such as Finance, Healthcare, and Technology, exhibit a distribution that is more skewed towards zero, suggesting the presence of resilience against cyber threats.

Figure 13: Distribution of changes in probability of default with respect to expected values 1 and 12 months after a cyber-event

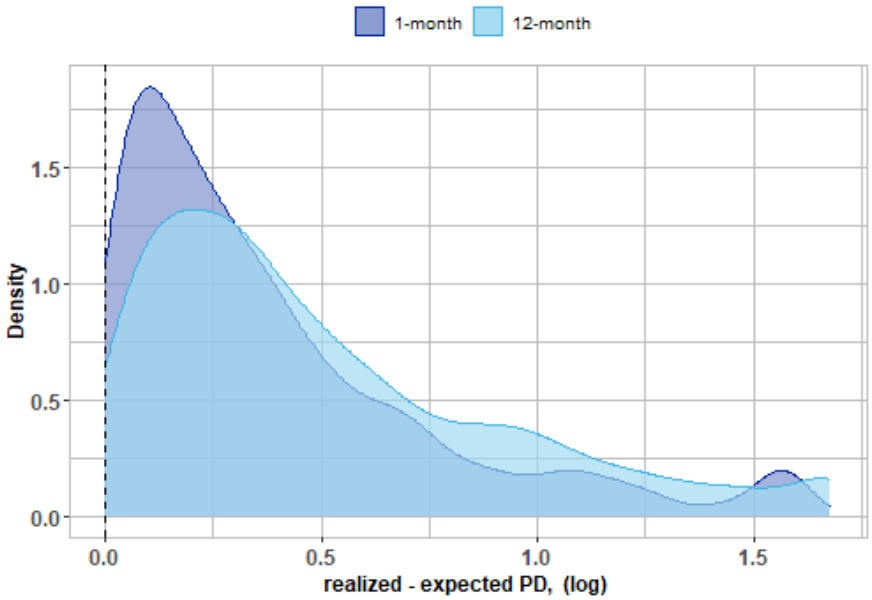
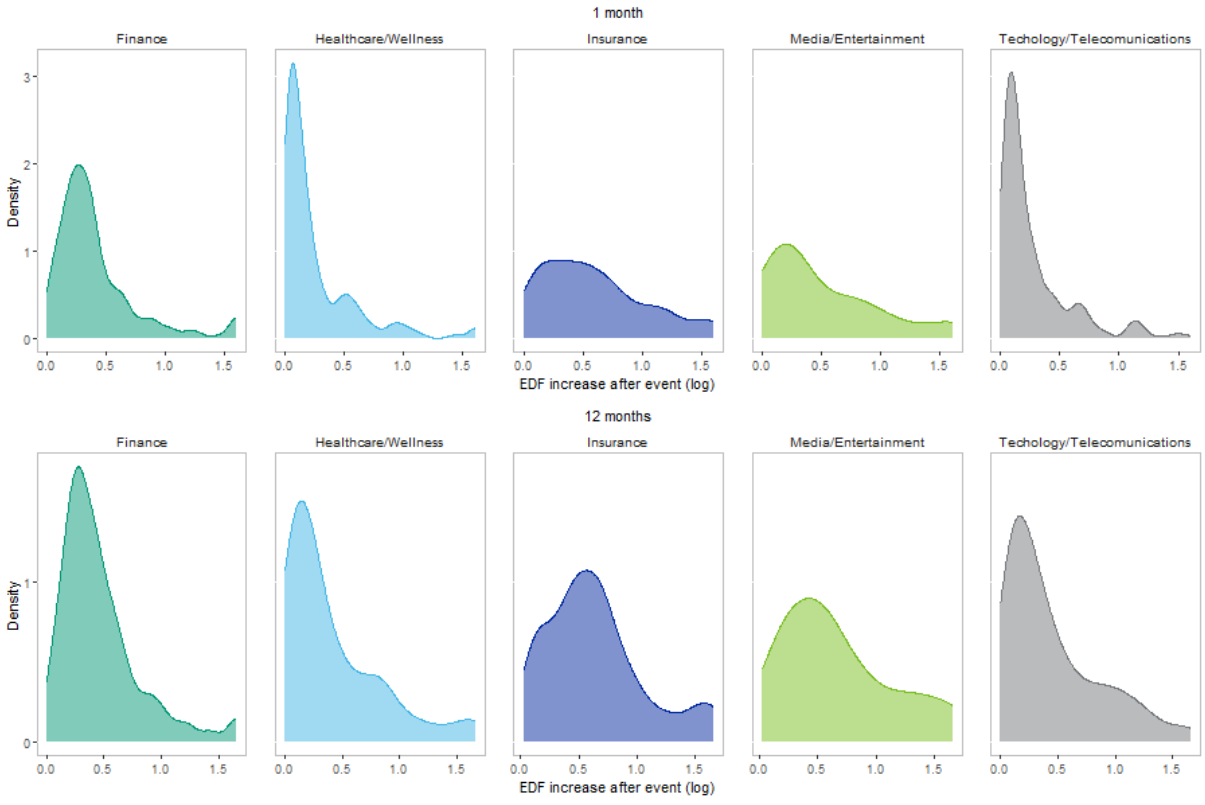



Figure 14: Distribution of changes in probability of default with respect to expected values 1 and 12 months after a cyber-event by industry.



## 5. Conclusion

Our study provides empirical evidence regarding the persistent nature of cybersecurity incidents and their financial implications. Given the sensitive and invaluable nature of the data they handle, organizations operating within these sectors must prioritize robust security measures and allocate ample resources to safeguard their assets effectively. We found that cybersecurity practices, as proxied by the Bitsight cybersecurity rating, are strongly correlated with the likelihood of a cyber incident. The statistically significant and negative coefficient associated with Bitsight's cybersecurity rating reinforces the imperative of ongoing evaluation and enhancement of cybersecurity measures to reduce the likelihood of adverse events.

Moreover, our study elucidates the significant negative impacts of cyber incidents on financial performance, as evidenced by the enduring negative equity returns experienced over a 12-month period following severe events. This finding points out the potentially persistent financial implications of cybersecurity breaches and emphasizes the urgency of swift and efficacious incident response strategies to mitigate potential damage to a company's market value.

Cyber events can disrupt a company's equity returns trajectory and exert a detrimental impact on its market asset value, thus potentially affecting its credit risk. These findings underscore the interconnected nature between cybersecurity and financial soundness, emphasizing the necessity for organizations to incorporate cyber risk management as an integral component of their broader risk management strategies.

Notably, our findings also unveil pronounced disparities in the impact of cyber incidents across different industries. While some industries such as Finance, Healthcare, and Technology sectors experience a higher frequency of attacks, they demonstrate a comparatively superior ability to mitigate the financial consequences of such incidents, resulting in lower average losses. This suggests that these industries have successfully implemented effective risk management practices and made substantial investments in cybersecurity measures to shield their assets and alleviate financial risks.

Taken all together, the results of our empirical analysis further emphasize the importance of cybersecurity as key component of an integrated risk assessment framework, alongside credit risk, operational risk, compliance, supply chain, and more. Developing a risk-aware culture, and supplying risk managers with the tools and data required to assess, monitor, communicate, and respond is needed. Our findings here indicate that those goals are both urgent and achievable.

## 6. References


Bitsight methodology paper. (2023) "Policy Review Board: How Bitsight Calculates Security Ratings."

Campbell, John Y., Andrew W. Lo and Archie Craig MacKinlay. "The Econometrics of Financial Markets." Princeton University Press, Princeton, NJ, 1997.

Pooya Nazeran, Dwyer, Douglas "Credit Risk Modeling of Public Firms: EDF9" *Moody's Analytics Model Methodology*, June 2015.

Dwyer, Douglas, Mateusz Giezek, Pineiro, Maitena, and Richard Loeser, "The Business Impact of ESG Performance." *Moody's Analytics Whitepaper*, June 2022.

MacKinlay, A. Craig, "Event Studies in Economics and Finance.", *Journal of Economic Literature*, Vol. XXXV, pp. 13–39, March 1997.

Pineiro, Maitena, Mateusz Giezek, Richard Loeser, David Zhong and Douglas Dwyer, "Measuring Persistence in ESG Incidents." *Moody's Analytics Whitepaper*, 2021.

## 7. Appendix

Details of the logistic regression model used to predict the probability of a cyber event are presented below. Table 5 shows that Bitsight's cybersecurity rating, together with log-sales (used as a proxy for firm size), are good predictors of whether a company will likely experience a cyber event. In particular, companies with a better cyber rating score tend to experience fewer events, whereas the larger the company, the more events take place.

Table 5: Probability of cyber event model

| Variable | Estimate | Std. Error | Pr(>\|z\|) | |
|---|---|---|---|---|
| Intercept | -3.1334 | 0.1773 | < 2e-16 | *** |
| Bitsight's cybersecurity rating | -0.0028 | 0.0002 | < 2e-16 | *** |
| Company size (in log sales) | 0.4928 | 0.0146 | < 2e-16 | *** |
| Industry fixed effects | … | … | … | |
| Seasonality effects | … | … | … | |

*Signif. codes: 0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

Figure 7 displays the ROC curve with an AUC of 0.80[10]. However, it should be noted that this is a largely imbalanced data set, as the history of publicly disclosed cyber events is relatively small. The model performs well in terms of being able to identify cyber events, but it suffers from a relatively high false positive rate (Type I errors) due to low precision.

Figure 7: Area under the receiver operator curve

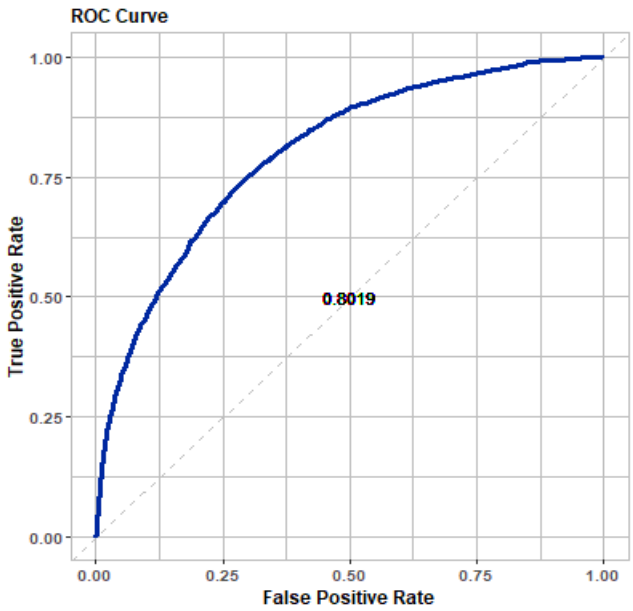



Figure 10 shows plots of how the average frequency of cyber events changes with the BitSight grade scale (from A, very good, to F, very bad). It can be seen that, in general, firms that receive the top grade, A, tend to suffer fewer cyber events.

[10] ROC: Receiver Operating Characteristic (ROC) is a statistical curve that illustrates the diagnostic ability of a binary classifier system. It plots the true positive rate (sensitivity) against the false positive rate (1 - specificity) at various threshold settings. AUC: Area Under the Curve (AUC) is a performance measurement for classification problem at various thresholds settings. It represents the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative one. AUC ranges in value from 0 to 1, where a higher score is a good indicator of a model's performance.

Figure 10: Average frequency of cyber event by risk vector grades